



E-Safety Policy



Our Goals

- Creating a safe learning environment to ensure students' safety while using the Internet.
- Increasing a general awareness about the benefits of using the Internet and the risks of its misuse on student growth and safety.
- Spreading the cultural awareness of cyber security.
- Enabling the students to use the Internet in a safe and smart way.
- Improving teachers' skills and capabilities so they can help and teach the students how to be responsible while using the Internet safely.
- Informing parents about the benefits of using the Internet and the consequent risks of its misuse.
- Encouraging the students to participate in raising the awareness of the safe use of the Internet in school and outside of the school.
- Perceiving the importance of social responsibility within the educational field.
- Creating a safe social environment for internet users.

The School Responsibilities

- Provide the administration, educational staff and students with technical support.
- Spreading the awareness of the importance and benefits of the internet as well as the dangers of its misuse among the school community and parents.
- Pledging a safe environment for the internet users in terms of using technology appropriately in the educational process.



- Maintaining the confidentiality of information related to the administration, educational staff, students and parents.
- Responding and solving all complaints and suggestions received through different electronic channels.
- Communicating and interacting with parents through the communication channels.
- Informing the parents of all e-security policies applied in the school, possible changes, and all the updates.

Parents (Guardians) Responsibilities

- Adhering to the school policies and guidelines on digital security.
- Not objecting to the school's decision against their children who violated the esecurity policies set by the school.
- Informing the school of any incident of bullying, fraud, or exploitation that any of their children was exposed to.
- Cooperating with the school to solve any accident that children were exposed to.



•

Monitoring the children's use of social media and explain explicitly the acceptable and unacceptable use of computers, networks, e-mails, and internet services.

- Empowering the community to adopt a healthy relationship with the means of modern technology and social media by supporting the capabilities of family members to interact positively with the digital world and raising the community awareness of the current challenges related to the digital safety and ways to prevent its risks.
- Reviewing the policy of the appropriate use of technology for students in the school, the Regulations of Students' Behavior (Distance Learning 2020) and the policy of using devices where the responsibility of violating the instructions is entirely on the student.

Please cooperate with the school administration to urge the student to abide by the given instructions.

Acceptable Use of Technology Policy for Students

- The school's acceptable use policy clarifies the rules that must be followed when using the computer, network, e-mail and internet services in accordance with the regulations and policies set by the country, the Sharjah Private Education Authority (SPEA) and the school to enhance e-safety in the school environment. The school also encourages everyone to take responsibility when using technology safely.
- The student is obligated to bring his electronic device to the school when needed, with a full commitment to appropriate use.
- The student must not download and upload any programs, games, music, graphics or videos.



- The student is not allowed to bring the mobile phone, smart watches, cameras, and all other electronic devices into the school except for the device specified by the school. The school is not responsible for any device that is damaged and lost in the school.
- The school provides students with access to platforms related to the education process that enhance knowledge acquisition and help them carry out their assignments.
- The school has the authority to monitor every activity that the student performs on educational platforms and websites.
- The student's online activities must comply with the school's policy and regulations.
- The e-mail, username and password are the responsibility of the student only, and he is fully responsible for any misuse recorded on it, with the need to change his password regularly, and not inform anyone about it, to stop others from accessing his device.
- The official school e-mail is used for official correspondence and should not be used personally, nor is the use of any other e-mail is acceptable.
- It is prohibited to use the internet to send, download or publish any offensive or inappropriate material that is against the laws, rules and regulations of the country and the school, or against morals or Islamic precepts.
- Never open e-mails or attachments from unknown sources.
- It is prohibited to impersonate others, use another student's personal account, or distribute private information about others or themselves when using the platforms and websites.
- It is forbidden to photograph or record teachers or students without permission to use devices such as mobile phones, tablets or cameras.
- Not to write or post abusive or inappropriate comments about students, teachers, or the school and harm them through various means or technological platforms.



•

- No student is allowed to enter suspicious websites to penetrate or download programs that could affect school devices, such as spreading viruses or sending messages that hinder or destroy these devices.

It is prohibited to commit any behavior that violates the school discipline regulation, including any kind of cyberbullying, and the school will take strict and disciplinary procedures to maintain a safe and disciplined atmosphere in the school.

- It is prohibited to download commercial software or any material protected by copyright and intellectual property without a license.
- The student is not allowed to disrupt the work of computers, school electronic systems, and the Internet, or destroy them in any way.
- The student using the school network should contact the complaints department in the school when any security problem is noticed and immediately report any security risks and violations.

The school has the authority to take the needed action, in accordance with the regulations and rules that are followed by Sharjah Private Education Authority (SPEA) and the school, against those who violate these policies.



Acceptable Use of Technology Policy for the Administration and Teaching Staff.

- The school's acceptable use policy clarifies the rules that must be followed when using the computer, network, e-mail and internet services in correspondence with the regulations and policies set by the country, the Sharjah Private Education Authority (SPEA) and the school to enhance digital security in the school environment.
The school also encourages everyone to take responsibility when using technology safely.
- The school facilitate a quick access to the internet for the teacher to help in carrying out the required tasks that are related to the education process only. The teacher bears the responsibility of using the internet.
- The school has the authority to monitor every activity that the teacher performs on educational platforms and websites.
- The e-mail, username and password are the responsibility of the teacher only, and he is fully responsible for any misuse recorded on it, with the need to change his password regularly.
- The official school e-mail is used for official correspondence and should not be used personally, nor is the use of any other e-mail is acceptable.



•

- The activities carried out by the employee on the internet must be in accordance with the policy and rules of Sharjah Private Education Authority (SPEA) and the school.
- Never open e-mails or attachments from unknown sources.
It is forbidden to impersonate others, use another person's personal account, or publish private information about others or themselves when using the platforms and websites.
- Not to write or post abusive or inappropriate comments regarding students, employees or the school and harm them through various means or technological platforms.
- It is prohibited to use the internet to send, download or publish any offensive or inappropriate material that is against the laws, rules and regulations of the country and the school, or against morals or Islamic precepts.
- No employee is allowed to enter suspicious websites to penetrate or download programs that could affect school devices, such as spreading viruses or sending messages that hinder or destroy these devices.
- It is prohibited to publish information about the school, teachers, students, and personal contact information through any means of communication or any website.
- Not to publish photos or videos of students on various websites without the school administration's permission.
- Providing staff with a cell phone from the school if their work requires it.
- It is prohibited to download commercial software or any material protected by copyright and intellectual property without a license.
- Mobile phones should not be used during the lessons.



- The teacher using the school network should contact the complaints department in the school when any security problem is noticed and immediately report any security risks, violations and any illegal material or content.

Reviewed on July 2022

